L18: Entry 2 of 2 File: DWPI Sep 17, 2002

DERWENT-ACC-NO: 1998-137649
DERWENT-WEEK: 200268

TITLE: Mobile communication system using roaming terminal - in which first decoding key provided in home network, is used for decoding encrypted terminal ID

INVENTOR: TOMOIKE, H

PATENT-ASSIGNEE:

ASSIGNEE	CODE
NEC CORP	NIDE

PRIORITY-DATA: 1996JP-0161647 (June 21, 1996)

Search Selected Search ALL Clear

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
SE 518284 C2	September 17, 2002		000	H04Q007/38
JP 10013945 A	January 16, 1998		009	H04Q007/38
SE 9702326 A	December 22, 1997		000	H04Q007/38
US 5940512 A	August 17, 1999		000	H04L009/32

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
SE 518284C2	June 18, 1997	1997SE-0002326	
JP 10013945A	June 21, 1996	1996JP-0161647	
SE 9702326A	June 18, 1997	1997SE-0002326	
US 5940512A	June 19, 1997	1997US-0879234	

INT-CL (IPC): H04 L 9/08; H04 L 9/30; H04 L 9/32; H04 Q 7/22; H04 Q 7/38

ABSTRACTED-PUB-NO: JP 10013945A
BASIC-ABSTRACT:

The system includes multiple roaming point networks other than a home network to which a roaming terminal (10) belongs. The roaming point networks receive mobile communication service offered in different areas by multiple stations.

When a terminal notifies a terminal ID to the home network through the roaming point network, a first encipherment key enciphers the ID. A first decoding key which performs decoding of the encrypted ID is provided in the home network.

ADVANTAGE - Avoids notification of inherent information relating to terminals, to roaming point network.

ABSTRACTED-PUB-NO:

US 5940512A
EQUIVALENT-ABSTRACTS:

The system includes multiple roaming point networks other than a home network to which a roaming terminal (10) belongs. The roaming point networks receive mobile communication service offered in different areas by multiple stations.

When a terminal notifies a terminal ID to the home network through the roaming point network, a first encipherment key enciphers the ID. A first decoding key which performs decoding of the encrypted ID is provided in the home network.

ADVANTAGE - Avoids notification of inherent information relating to terminals, to roaming point network.

CHOSEN-DRAWING: Dwg.1/5

TITLE-TERMS: MOBILE COMMUNICATE SYSTEM TERMINAL FIRST DECODE KEY HOME NETWORK DECODE ENCRYPTION TERMINAL ID

DERWENT-CLASS: W01 W02

EPI-CODES: W01-A05A; W01-B05A1A; W01-C02B6A; W02-C03C1A;

SECONDARY-ACC-NO:
Non-CPI Secondary Accession Numbers: N1998-109473

Previous Doc Next Doc Go to Doc#

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平10－13945
(43)公開日　平成10年(1998)１月16日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｑ	7/38			Ｈ０４Ｂ	7/26	１０９Ｈ
Ｈ０４Ｌ	9/30			Ｈ０４Ｌ	9/00	６６３Ｚ
	9/32					６７３Ｂ
						６７３Ｃ

審査請求　有　請求項の数９　ＯＬ　（全９頁）

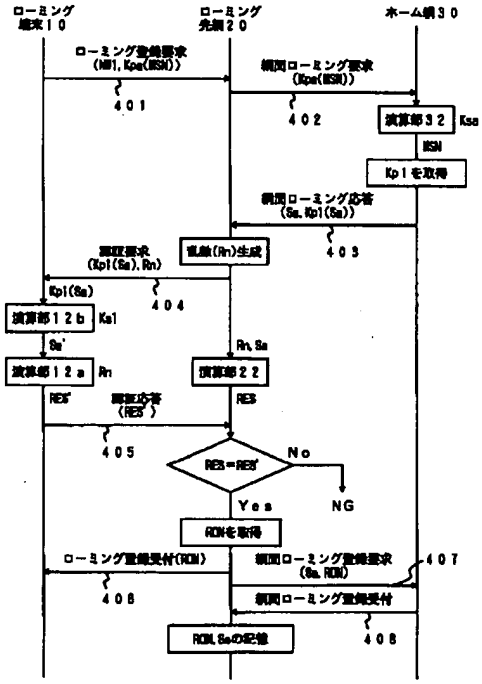
(21)出願番号　特願平8－161647

(22)出願日　平成８年(1996)６月21日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　友池　裕元
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　弁理士　後藤　洋介　（外２名）

(54)【発明の名称】　ローミング方式

(57)【要約】
【課題】　加入者番号や、認証鍵等の端末に関する固有情報をローミング先網に通知することなく、ローミング処理を行うことできるローミング方式を提供する。
【解決手段】　ローミング端末１０は、加入者番号ＭＳＮをホーム網の公開鍵Ｋpaで暗号化し、ローミング先網２０を介してホーム網３０へ送信する。ホーム網３０は秘密鍵Ksaで暗号を解読してＭＳＮを得、一時的に生成した認証鍵Ｓa をＭＳＮに対応する端末の公開鍵Ｋp1で暗号化する。認証鍵Ｓa がローミング先網に通知され、暗号化された認証鍵がローミング端末に通知されると、ローミング先網が発生した乱数とこれら認証鍵を用いて端末の認証が行われる。認証が終了するとローミング先網はローミング番号を獲得し、ローミング端末及びホーム網に通知する。ローミング端末、ローミング先網、及びホーム網は、それぞれローミング番号と認証鍵とを記憶する。



1

【特許請求の範囲】

【請求項１】　複数の事業者がそれぞれ異なる地域で提供する移動通信サービスを、端末が所属するホーム網以外のローミング先網で受けるためのローミング方式において、前記端末に第１の暗号化鍵を与えるとともに、前記ホーム網に前記暗号化鍵により暗号化された情報を復号する第１の復号鍵を与え、前記端末がローミング先網を介して前記ホーム網へ該端末のＩＤを通知する際に、前記端末において前記ＩＤを前記第１の暗号化鍵を用いて暗号化し、前記ホーム網において前記第１の復号鍵を用いて暗号化されたＩＤを復号するようにしたことを特徴とするローミング方式。

【請求項２】　前記第１の暗号化鍵が公開鍵であり、前記第１の復号鍵が秘密鍵であることを特徴とする請求項１のローミング方式。

【請求項３】　前記ホーム網に第２の暗号化鍵を与えるとともに、前記端末に前記第２の暗号化鍵により暗号化された情報を復号する前記第２の復号鍵を与え、前記ホーム網で生成した認証鍵を前記ローミング先網へ送信するとともに、前記認証鍵を前記第２の暗号化鍵で暗号化して前記ローミング先網を介して前記端末へ送信し、前記端末において前記第２の復号鍵を用いて暗号化された認証鍵を復号するようにしたことを特徴とする請求項１または２のローミング方式。

【請求項４】　前記ローミング先網が乱数を発生し、該乱数を前記暗号化された認証鍵とともに前記端末へ送信し、前記端末において前記乱数と前記第２の復号鍵で復号した認証鍵との演算処理を行って得た演算結果を前記ローミング先網へ返送させ、前記ローミング先網で前記乱数と前記認証鍵との演算処理を行った結果と前記演算結果と比較することにより、認証処理を行うことを特徴とする請求項３のローミング方式。

【請求項５】　前記第２の暗号化鍵が公開鍵であり、前記第２の復号鍵が前記端末に固有の秘密鍵であることを特徴とする請求項３または４のローミング方式。

【請求項６】　前記ホーム網及び前記ローミング先網における前記端末に関するローミング登録を、前記ローミング先網が前記端末に割り当てるローミング番号と前記認証鍵とを用いて行うようにしたことを特徴とする請求項３、４、または、５のローミング方式。

【請求項７】　複数の事業者がそれぞれ異なる地域で提供する移動通信サービスを、端末が所属するホーム網以外のローミング先網で受けることができる移動通信システムにおいて、前記端末が、ローミング時に、自身のＩＤを第１の暗号化鍵で暗号化し、前記ホーム網の網番号とともに、ローミング登録要求信号に含ませて送信する手段と、受信した認証要求信号に含まれる第２の暗号化鍵で暗号化された認証鍵を解読する手段と、受信したローミング受付信号に含まれるローミング番号と前記認証鍵とを関連付けて記憶する記憶手段とを備え、前記前記

2

ローミング先網が、前記ローミング登録要求信号を受信して、前記網番号が示す前記ホーム網へ前記暗号化されたＩＤを含む網間ローミング要求信号を送信する手段と、前記ホーム網からの網間ローミング応答信号に含まれる認証鍵と、前記端末に割り当てるローミング番号とを関連付けて記憶する記憶する手段と、前記網間ローミング応答信号に含まれる第２の暗号化鍵で暗号化された認証鍵を前記認証要求信号として前記端末へ送信する手段と、前記ローミング番号を前記端末及び前記ホーム網へ送信する手段と、前記ホーム網が、前記網間ローミング要求信号を受信し、前記暗号化されたＩＤを解読する手段と、前記認証鍵を生成し、該認証鍵を前記ＩＤに対応する前記第２の暗号化鍵で暗号化し、前記認証鍵と前記暗号化された認証鍵とを含む前記網間ローミング応答信号を送信する手段と、前記ローミング番号を前記ＩＤに関連させて記憶する記憶手段とを有することを特徴とする移動通信システム。

【請求項８】　前記ローミング先網が、前記認証要求信号に含めて送信される乱数を生成する乱数生成手段と、前記乱数と前記認証鍵との演算を行う演算手段と、該演算手段の出力と前記端末からの認証応答信号とを比較する比較手段と、該比較手段の比較結果が一致したとき前記端末にローミング番号を割り当てる手段とを有し、前記端末が、前記乱数と前記復号した認証鍵との演算を行う演算手段と、該演算手段の演算結果を前記認証応答信号として前記ローミング先網へ送信する手段とを有することを特徴とする移動通信システム。

【請求項９】　前記第１の暗号化鍵が前記ホーム網固有の公開鍵であり、前記第２尾暗号化鍵が前記端末固有の公開鍵であることを特徴とする請求項７または８の移動通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ローミング方式に関し、特に、移動通信端末が、契約した事業者以外の事業者のサービスエリアへ移動したときのローミング方式に関する。

【０００２】

【従来の技術】移動通信の分野では、複数の事業者が、それぞれ異なる地域で各々のサービスを提供している。そして、いずれかの事業者と契約した移動通信端末であって、他の事業者の提供するサービスエリアでもにおいて、自端末が契約した事業者のサービスエリア内に位置する場合と同様のサービスが受けられるよう、これら複数の事業者は、ローミングサービスを行っている。

【０００３】図５を参照して、従来の移動端末ローミング方式における、ローミング端末の登録手順を説明する。ローミング端末は、無線基地局からの報知情報を受信しており、その報知情報から、網間ローミングをしたことを知る。つまり、自端末が契約しているホーム網の

サービスエリアを出て、他の事業者（ローミング先網）のサービスエリアに入ったことを知る。そして、ローミング端末は、ローミング先網に対して位置登録要求信号５０１を送信する。この位置登録要求信号５０１には、加入者ＩＤである加入者番号（以下、ＭＳＮ）が含まれている。

【０００４】ローミング先網（の交換局）では、ローミング端末からの位置登録要求信号５０１を受信すると、それに含まれるＭＳＮによって、その端末がローミング端末であると認識する。そして、ローミング先網は、認証処理を行うために、ＭＳＮから知得したホーム網に対して網間認証情報読出要求信号５０２を送信する。この網間認証情報読出要求信号５０２には、ＭＳＮが含まれる。また、ローミング先網は、ローミング端末に対して認証要求信号５０３を送信する。この認証要求信号５０３には、ローミング先網内で生成した認証乱数が含まれる。

【０００５】ホーム網（の交換局）は、自網に所属する端末の認証に必要な認証キーを全て記憶しており、網間認証情報読出要求信号５０２を受信すると、その信号に含まれるＭＳＮが付与された端末の認証キーを検索する。そして、検索した認証キーを網間認証情報読出応答信号５０４でローミング先網へ通知する。

【０００６】また、ローミング端末は、ローミング先網から認証要求信号５０３を受信すると、その認証要求信号５０３に含まれる認証乱数と自信で記憶している固有の認証キーとの演算を、演算回路を用いて行い、その演算結果を認証応答信号５０５でローミング先網に返送する。

【０００７】ローミング先網では、ホーム網からの網間認証情報読出応答信号５０４により得た認証キーと、先にローミング端末へ送信したのと同じ認証乱数との演算処理を行う。そして、ローミング先網は、その演算結果とローミング端末からの認証応答信号５０５に含まれる認証演算結果とを比較する。これらの結果が一致していれば、ローミング端末は、ホーム網に登録されている端末であると判定される。即ち、認証ＯＫとなる。そして、ローミング先網は、そのローミング端末に付与すべきローミング番号（ＲＯＭ）を捕捉し、ＲＯＭを含む位置登録受付信号５０６をローミング端末に送信する。また、ローミング先網は、ＭＳＮ及びＲＯＮを含む網間位置登録要求信号５０７をホーム網へ送信する。

【０００８】ホーム網は、ローミング先網から網間位置登録要求信号５０７を受信すると、その信号に含まれるＭＳＮ及びＲＯＮを記憶する。そして、ＭＳＮに対応する端末に関する情報、例えば、加入者情報、認証キー等を、網間位置登録応答信号５０８により送信する。

【０００９】ローミング先網は、ホーム網から送信されてきた網間位置登録応答信号５０８に含まれる加入者情報及び認証キー等の情報をローミング端末に割り当てたＲＯＮとともに記憶する。

【００１０】上記のようにして、従来のローミング方式では、ローミング端末の登録処理が行われる。これより以後、ローミング端末の位置登録時、発呼時の呼処理は、ローミング先網と、ローミング端末との間で、直接行われる。

【００１１】以上説明したように、従来のローミング処理では、ローミング端末の認証処理を効率良く行うために、初回のローミング登録時に、当該ローミング端末の認証キーをホーム網からローミング先網へ転送している。このため、従来のローミング方式には、認証キーをローミング先網に知られてしまい、漏洩などの危険がある等、セキュリティの面で問題がある。

【００１２】この問題を解決する方法として、特開平４－３５２５２５号公報に開示された方法がある。これは、まず、ローミング端末から位置登録要求を受けたローミング先網が、ローミング処理に使用する仮認定鍵を生成してホーム網に送信しておく。ホーム網は、ローミング先網を経由してローミング端末の認証を行う。ホーム網は、ローミング端末が保持する仮認証鍵設定鍵と同一の鍵を保持しており、認証終了後、この鍵を用いて仮認定鍵を暗号化し、ローミング先網を経由してローミング端末へ送る。ローミング端末は、暗号化された仮認定鍵を、仮認証鍵設定鍵により解読して、仮認証鍵を得る。以降、ローミング先網との認証処理には、この仮認証鍵を使用する。こうして、ローミング先網に、認証鍵を知られることなく、ローミング処理（認証処理）を行うことができる。

【００１３】

【発明が解決しようとする課題】従来のローミング方式では、ローミング端末が位置登録要求を行うには、まず、加入者番号（ＭＳＮ）を、ローミング先網へ送信しなければならない。ローミング端末は、当然、その送信を無線によって行うので、傍受される恐れがあり、ローミング端末の匿名性を確保することができないという問題点がある。

【００１４】本発明は、加入者番号や、認証鍵等の端末固有の情報をローミング先網に通知することなく、ローミング処理を行うことできるローミング方式を提供することを目的とする。

【００１５】また、本発明は、セキュリティの高い移動通信システムを構築することを目的とする。

【００１６】

【課題を解決するための手段】本発明によれば、複数の事業者がそれぞれ異なる地域で提供する移動通信サービスを、端末が所属するホーム網以外のローミング先網で受けるためのローミング方式において、前記端末に第１の暗号化鍵を与えるとともに、前記ホーム網に前記暗号化鍵により暗号化された情報を復号する第１の復号鍵を与え、前記端末がローミング先網を介して前記ホーム網

5

へＩＤを通知する際に、前記端末において前記ＩＤを前記第１の暗号化鍵を用いて暗号化して通知し、前記ホーム網において前記第１の復号鍵を用いて暗号化されたＩＤを復号するようにしたことを特徴とするローミング方式。

【００１７】また、本発明によれば、前記ホーム網に第２の暗号化鍵を与えるとともに、前記端末に前記第２の暗号化鍵により暗号化された情報を復号する前記第２の復号鍵を与え、前記ホーム網で生成した認証鍵を前記ローミング先網へ送信するとともに、前記認証鍵を前記第２の暗号化鍵で暗号化して前記ローミング先網を介して前記端末へ送信し、前記端末において前記第２の復号鍵を用いて暗号化された認証鍵を復号するようにしたことを特徴とするローミング方式が得られる。

【００１８】さらに本発明のよれば、前記ローミング先網が乱数を発生し、該乱数と前記暗号化された認証鍵とを前記端末へ送信し、前記端末において前記乱数と前記第２の復号鍵で復号した認証鍵との演算処理をおこなって演算結果を前記ローミング先網へ返送させ、前記ローミング先網で前記乱数と前記認証鍵との演算処理を行い前記演算結果と比較することにより、認証処理を行うことを特徴とするローミング方式が得られる。

【００１９】さらにまた、本発明によれば、複数の事業者がそれぞれ異なる地域で提供する移動通信サービスを、端末が所属するホーム網以外のローミング先網で受けることができる移動通信システムにおいて、前記端末が、ローミング時に、自身のＩＤを第１の暗号化鍵で暗号化し、前記ホーム網の網番号とともに、ローミング登録要求信号に含ませて送信する手段と、受信した認証要求信号に含まれる第２の暗号化鍵で暗号化された認証鍵を解読する手段と、受信したローミング受付信号に含まれるローミング番号と前記認証鍵とを関連付けて記憶する記憶手段とを備え、前記前記ローミング先網が、前記ローミング登録要求信号を受信して、前記網番号が示す前記ホーム網へ、前記暗号化されたＩＤを含む網間ローミング要求信号を送信する手段と、前記ホーム網からの網間ローミング応答信号に含まれる認証鍵と、前記端末に割り当てるローミング番号とを関連付けて記憶する記憶する手段と、前記網間ローミング応答信号に含まれる第２の暗号化鍵で暗号化された認証鍵を前記認証要求信号として前記端末へ送信する手段と、前記ローミング番号を前記端末及び前記ホーム網へ送信する手段と、前記ホーム網が、前記網間ローミング要求信号を受信し、前記暗号化されたＩＤを解読する手段と、前記認証鍵を生成し、該認証鍵を前記ＩＤに対応する前記第２の暗号化鍵で暗号化し、前記認証鍵と前記暗号化された認証鍵とを含む前記網間ローミング応答信号を送信する手段と、前記ローミング番号を前記ＩＤに関連させて記憶する記憶手段とを有することを特徴とする移動通信システムが得られる。

6

【００２０】

【作用】ローミング端末からのローミング登録要求信号に含まれるＭＳＮは、ホーム網の公開鍵により暗号化されている。このため、ローミング端末のＭＳＮは、ローミング先網を含め第三者に知られることはない。

【００２１】また、ローミング端末とローミング先網との間の認証処理に使用される認証鍵は、ホーム網で生成されるもので、ローミング端末固有のものではない。しかも、ローミング先網からローミング端末への通知は、ローミング端末固有の公開鍵で暗号化された状態で行われるので、ローミング先網以外の第三者に知られることはない。

【００２２】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態について説明する。まず、図１乃至図３を参照して、本発明のローミング方式を採用する、ローミング端末、ローミング先網、及びホーム網の構成について説明する。

【００２３】図1は、ローミング端末１０のブロック図である。このローミング端末１０は、読み出し専用メモリ（以下、ＲＯＭ）１１ａと書き込み可能なメモリ（以下、ＲＡＭ）１１ｂ、第１の演算部１２ａと第２の演算部１２ｂ、及び無線送受信部１３を有している。また、これらを制御する図示しない制御部を有している。

【００２４】ＲＯＭ１１ａは、その端末に割り当てられた加入者（ＩＤ）番号（以下、ＭＳＮ）と、端末固有の秘密鍵、ホーム網の網番号、及びホーム網の公開鍵等を記憶している。ＲＡＭ１１ｂは、ローミング処理を行う際に、ホーム網から配送される認証鍵を記憶する。また、第１の演算部１２ａは、公開鍵認証方式による演算を行い、第２の演算部１２ｂは、秘密鍵認証方式による演算を行う。

【００２５】図2は、ローミング先網（交換局）２０のブロック図である。このローミング先網２０は、在圏ロケーションレジスタ（以下、ＶＬＲ）２１、演算部２２、無線送受信部２３ａ、通信制御部２３ｂ、呼制御部２４、ＰＮ発振部２５、及び比較部２６を有している。

【００２６】ＶＬＲ２１は、ローミング加入者のローミング番号（以下、ＲＯＮ）、認証鍵、及び位置情報等を格納する。演算部２２は、ローミング端末１０の第１の演算部１２ａと同一のアルゴリズムで、秘密鍵認証方式の演算処理を行う。無線送受信部２３ａは無線基地局（図示せず）とのインタフェース、通信制御部２３ｂは、ローミング端末１０のホーム網を含む他の網とのインタフェースである。また、呼制御部２４は、端末との間のローミング処理、認証処理等の呼制御を行う。ＰＮ発振部２５は、乱数を発生する。比較部２６は、認証結果の判定を行う。

【００２７】図3は、ローミング端末１０のホーム網（交換局）のブロック図である。このホーム網３０は、

ホームロケーションレジスタ（以下、HLR）31a、RAM31b、演算部32、通信制御部33、呼制御部34、及び認証鍵生成部35を有している。

【0028】HLR31aは、自網に所属する複数の端末（ローミング端末を含む）のMSNや、各端末の公開鍵等を記憶している。RAM31bは、ホーム網30の秘密鍵を記憶している。演算部32は、ローミング端末10の演算部12bと同一のアルゴリズムで、公開鍵認証方式の演算処理を行う。通信制御部33は、ローミング先網20を含む他網とのインタフェースである。呼制御部34は、呼の処理を行う。認証鍵生成部35は、ローミング端末10とローミング先網20との間の認証処理に使用される認証鍵を生成する。

【0029】以下、これら、ローミング端末10、ローミング先網20、及びホーム網30を含むシステムにおける、ローミング方式について、図4をも参照して説明する。

【0030】移動通信端末は、移動通信サービスが提供されているエリア内にいるときは、常時移動通信網から送られてくる報知情報により、自端末が存在する位置を認識している。したがって、移動通信端末は、自端末が契約した事業者以外の事業者が提供するサービスエリア内に入ったこと、即ち、ローミング端末10となったことを認識できる。

【0031】ローミング端末10の制御部は、報知情報により自端末が、ローミング先網20へローミングしたことを認識すると、ROM11aから、ホーム網の網番号（以下、NW1）、MSN、及びホーム網の公開鍵（以下、Kpa）を読み出す。そして、演算部12bに、MSNとKpaとを用いた公開鍵認証演算を実行させ、演算結果｛以下、Kpa（MSN）｝を得る。即ち、演算部12bは、Kpaを用いて、MSNを暗号化し、Kpa（MSN）を得る。そして、制御部は、無線送受信部13を介して、ローミング先網20に対し、NW1及びKpa（MSN）を含むローミング登録要求信号401を送出する。

【0032】ローミング先網20では、呼制御部24が、無線送受信部23aを介してローミング登録要求信号401を受信する。そして、呼制御部24は、ローミング登録要求信号401に含まれるNW1より、ローミング端末10のホーム網が、ホーム網30であることを認識する。そして、呼制御部24は、受信したローミング登録要求信号401に含まれていたKpa（MSN）を含む網間ローミング要求信号402を、ホーム網30へ送出する。

【0033】ホーム網30では、呼制御部34が、通信制御部33を介して網間ローミング要求信号402を受信する。呼制御部34は、網間ローミング要求信号402を受信すると、RAM31bからホーム網の秘密鍵（以下、Ksa）を読み出し、受信したKpa（MSN）とともに演算部32へ供給する。演算部32は、Kpa（MSN）とKsaとで公開鍵認証演算処理を行う。つまり、演算部32は、暗号Kpa（MSN）をKsaを用いて解読し、ローミング端末10のMSNを得る。呼制御部34は、演算部32で得たMSNに基づいて、ローミング端末10の公開鍵Kp1を、HLR31aから取り出す。同時に、呼制御部34は、認証鍵生成部35に対して認証鍵の生成を指示する。認証鍵生成部35は、呼制御部34からの指示により、任意の方法で、一時的な認証鍵（以下、Sa）を生成して、呼制御部34へSaを通知する。

【0034】続いて、呼制御部34は、上記のようにして得たKp1とSaを演算部32に通知する。演算部32は、Kp1とSaとで公開鍵演算処理を行い、演算結果｛以下、Kp1（Sa）｝を得る。即ち、演算部32は、Saを Kp1で暗号化する。呼制御部34は、このKp1（Sa）と、元のSaとを含む網間ローミング応答信号403を、通信制御部33を介してローミング先網20へ返送する。

【0035】ローミング先網20では、ホーム網30から網間ローミング応答信号403が返送されてくると、呼制御部24が、Kp1（Sa）とSaとを取り出す。そして、呼制御部24は、Kp1（Sa）とPN発振部25で生成した乱数Rnとを含む認証要求信号404をローミング端末10に対して送出する。

【0036】ローミング端末10では、認証要求信号404を受信すると、制御部は、ROM11aから固有の秘密鍵（以下、Ks1）を読み出す。そして、演算部12bに、Kp1（Sa）とKs1との演算処理を実行させる。つまり、演算部12bは、Ks1を用いてKp1（Sa）を解読し、演算結果（以下、Sa'）を得る。さらに制御部は、得られたSa'と、先に受信した乱数Rnとを用いた演算処理を演算部12aに実行させる。換言すると、演算部12aは、乱数Rnを Sa'で暗号化し、演算結果RES'を得る。制御部は、このRES'を認証応答信号405として、無線送受信部13を介してローミング先網20に送信する。

【0037】ローミング先網20では、認証要求信号404を送信したあと、演算部22により、乱数Rnと、認証鍵Saとの演算処理が行われ、演算結果RESが求められる。この演算結果RESは、比較部26に与えられ、ローミング端末10から送信されてくる認証応答信号405に含まれる演算結果RES'と比較される。比較の結果、これらが一致した場合は、呼制御部24は、認証OKと判定し、VLR21に、ローミング端末10に対するRONの割り当てを指示する。また、不一致の場合、呼制御部24は、認証NGと判定して、呼接続処理を中止する。

【0038】VLR21からRONの通知を受けた呼制御部24は、無線送信部23aを介して、RONを含む

ローミング登録受付信号４０６を、ローミング端末１０へ送信する。また、呼制御部２４は、ＲＯＮとＳａ とを含む網間ローミング登録要求信号４０７を、通信制御部２３ｂを介してホーム網３０へ送信する。

【００３９】ローミング端末１０では、ローミング登録受付信号４０６を受信すると、制御部が、受信した信号に含まれるＲＯＮと、先の演算で求めたＳａ'とをＲＡＭ１１ｂに格納する。

【００４０】ホーム網３０では、網間ローミング登録要求信号４０７を受信すると、呼制御部３４が、この信号に含まれるＳａ とＲＯＮとを、先のＭＳＮに関連付けてＨＬＲ２１に格納する。そして、呼制御部３４は、登録を受け付けたことを示す網間ローミング登録受付信号４０８を、ローミング先網２０へ送信する。

【００４１】ローミング先網２０の呼制御部２４は、網間登録受付信号４０８を受信すると、ＲＯＮとＳａ とをＶＬＲ２１に格納する。

【００４２】以上のようにして、ローミング端末の登録処理（ローミング処理）は完了する。このあと、ローミング端末１０からの発信時、及び、ローミング端末１０への着信時における接続処理は、以下のように行われる。

【００４３】ローミング端末１０から発信（発呼）を行う場合、ローミング端末１０は、ＲＯＮを含む発信要求信号を、ローミング先網２０へ送出する。

【００４４】ローミング先網２０は、端末からの発信要求信号を受信すると、この信号に含まれるＲＯＮにより、発呼を要求している端末が、ローミング端末であることを認識する。そして、ローミング先網２０は、ＶＬＲ２１より、ＲＯＮに対応する端末の認証鍵Ｓａ を取り出し、この認証鍵Ｓａ を用いて認証処理を行う。そして、認証処理が正常に終了した後、呼接続処理に移行する。

【００４５】また、ローミング端末１０への着信があった場合、ホーム網３０は、ＨＬＲ３１ａに格納されているＲＯＮから、該当する端末がローミング中であることを認識する。そして、ホーム網３０は、ローミング先網２０へ着呼を通知する。この通知に使用される通知信号の着信アドレスには、ＲＯＮが設定される。

【００４６】ローミング先網２０は、ホーム網３０からの通知信号に基づいて、ＶＬＲ２１から、ＲＯＮに対応する端末の位置情報、認証鍵Ｓａ 等の情報を取り出し、着信接続処理を行う。

【００４７】

【発明の効果】本発明のよれば、ローミング端末から、ローミング先網を介してホーム網へ送信されるＭＳＮをホーム網の公開鍵で暗号化して送信するようにしたことで、無線区間で傍受されてもＭＳＮが露呈することがない。しかも、ローミング先網に対しても秘密にすることができる。

【００４８】また、ホーム網からローミング先網へ送信される認証鍵は、端末に固有のものではなく、ホーム網で一時的に生成したものなので、ローミング先網で認証鍵が漏洩したとしても、セキュリティ上の大きな問題とはならない。

【図面の簡単な説明】

【図１】本発明のローミング方式が適用されるローミング端末のブロック図である。

【図２】本発明のローミング方式が適用されるローミング先網のブロック図である。

【図３】本発明のローミング方式が適用されるホーム網のブロック図である。

【図４】本発明のローミング方式の一実施の形態を示す図である。

【図５】従来のローミング方式のローミング端末登録処理の手順を説明するための図である。

【符号の説明】

１０	ローミング端末
１１ａ	読み出し専用メモリ（ＲＯＭ）
１１ｂ	書き込み可能なメモリ（ＲＡＭ）
１２ａ	第１の演算部
１２ｂ	第２の演算部
１３	無線送受信部
２０	ローミング先網
２１	在圏ロケーションレジスタ（ＶＬＲ）
２２	演算部
２３ａ	無線送受信部
２３ｂ	通信制御部
２４	呼制御部
２５	ＰＮ発振部
２６	比較部
３０	ホーム網
３１ａ	ホームロケーションレジスタ（ＨＬＲ）
３１ｂ	ＲＡＭ
３２	演算部
３３	通信制御部
３４	呼制御部
３５	認証鍵生成部
４０１	ローミング登録要求信号
４０２	網間ローミング要求信号
４０３	網間ローミング応答信号
４０４	認証要求信号
４０５	認証応答信号
４０６	ローミング登録受付信号
４０７	網間ローミング登録要求信号
４０８	網間ローミング登録受付信号
５０１	位置登録要求信号
５０２	網間認証情報読出要求信号
５０３	認証要求信号
５０４	網間認証情報読出応答信号

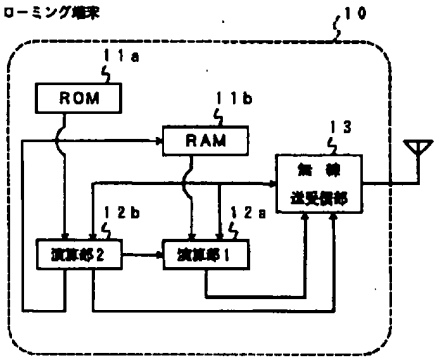
11

505　認証応答信号
506　位置登録受付信号

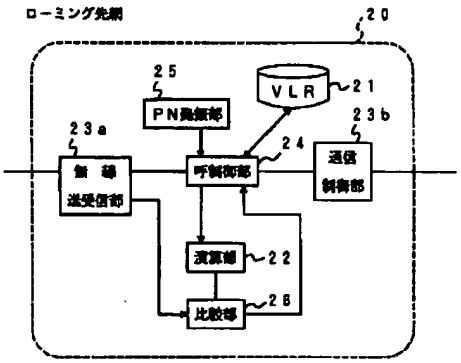
12

507　網間位置登録要求信号
508　網間位置登録応答信号

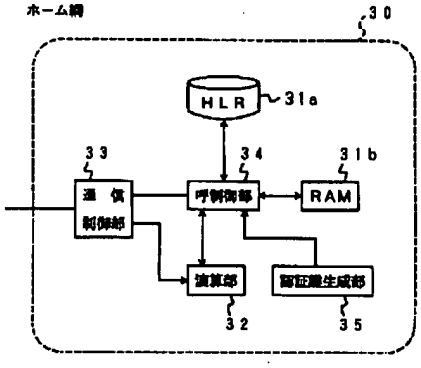
【図1】



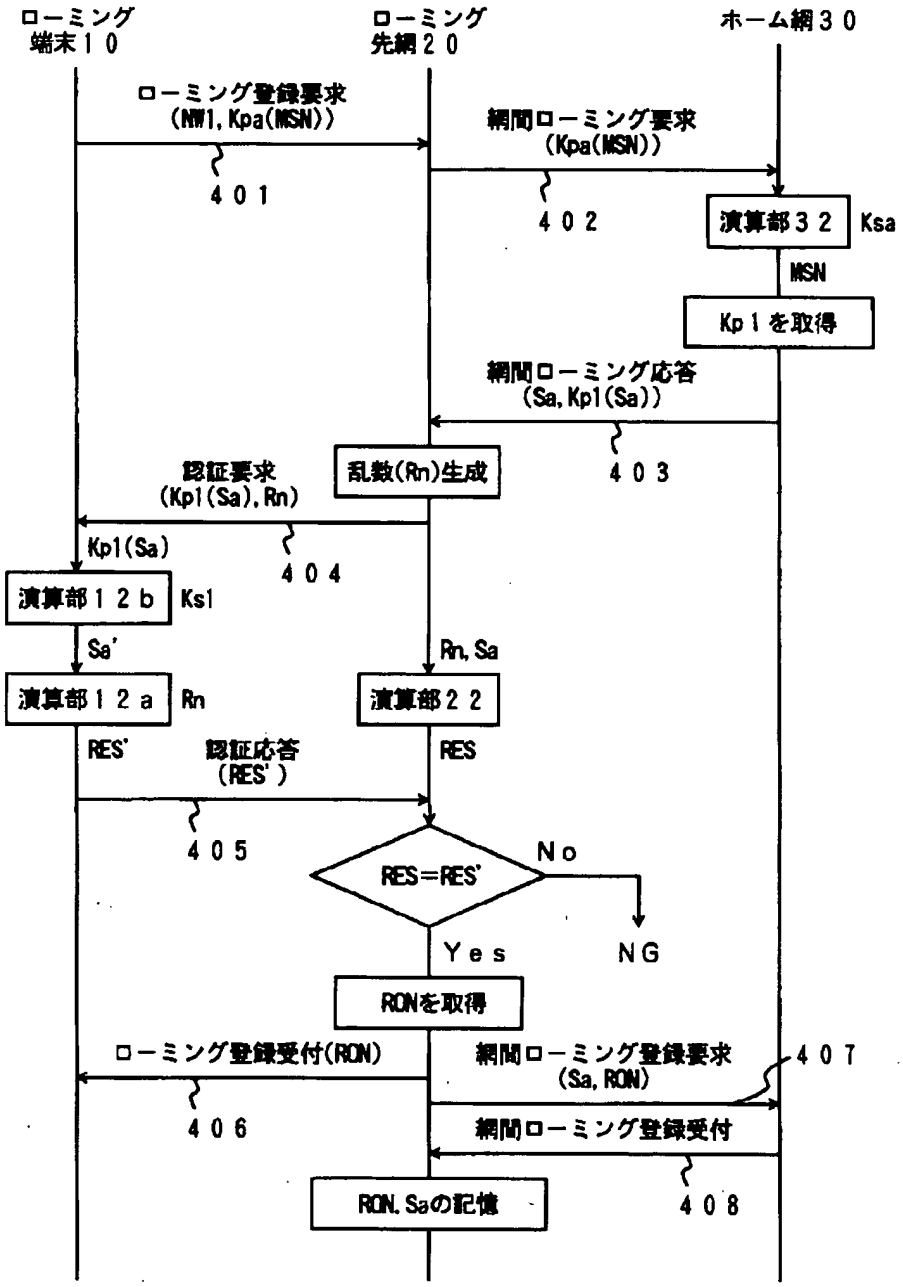
【図2】



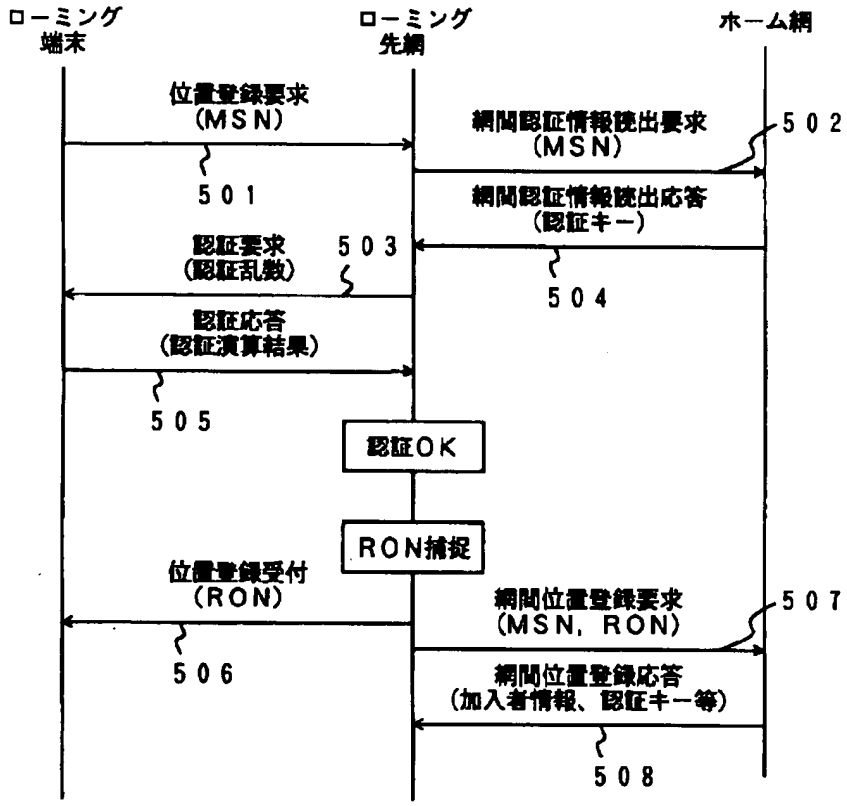
【図3】



【図4】


ローミング
端末10
ローミング
先網20
ホーム網30
ローミング登録要求
(NW1, Kpa(MSN))
401
網間ローミング要求
(Kpa(MSN))
402
演算部32
Ksa
MSN
Kp1を取得
網間ローミング応答
(Sa, Kp1(Sa))
403
乱数(Rn)生成
認証要求
(Kp1(Sa), Rn)
404
Kp1(Sa)
演算部12b
Ks1
Sa'
Rn, Sa
演算部12a
Rn
演算部22
RES'
認証応答
(RES')
RES
405
RES=RES'
No
NG
Yes
RONを取得
ローミング登録受付(RON)
406
網間ローミング登録要求
(Sa, RON)
407
網間ローミング登録受付
408
RON, Saの記憶

【図5】


ローミング
端末
ローミング
先網
ホーム網
位置登録要求
(MSN)
501
網間認証情報読出要求
(MSN)
502
網間認証情報読出応答
(認証キー)
504
認証要求
(認証乱数)
503
認証応答
(認証演算結果)
505
認証OK
RON捕捉
位置登録受付
(RON)
506
網間位置登録要求
(MSN, RON)
507
網間位置登録応答
(加入者情報、認証キー等)
508

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-013945

(43)Date of publication of application : 16.01.1998

(51)Int.Cl. H04Q 7/38
H04L 9/30
H04L 9/32

(21)Application number : 08-161647

(22)Date of filing : 21.06.1996

(71)Applicant : NEC CORP

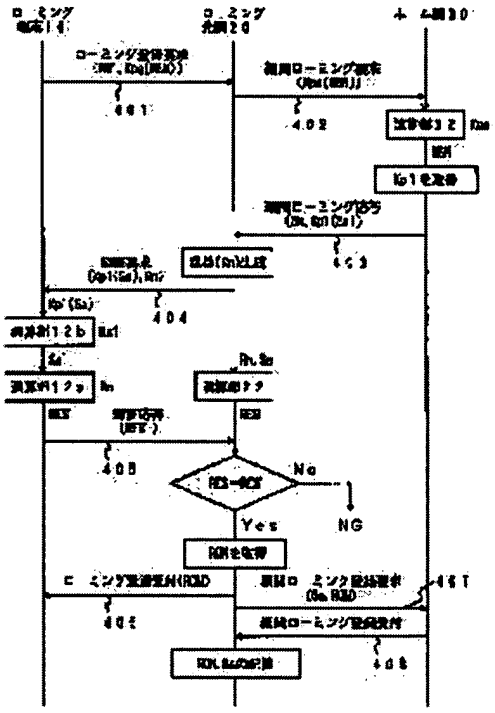
(72)Inventor : TOMOIKE HIROMOTO

(54) ROAMING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a roaming system which can perform roaming processing, without notifying proper information about a subscriber number and a terminal of an authentication key, etc., to a roaming bound network.

SOLUTION: A roaming terminal 10 encrypts a subscriber number MSN with a public key Kpa of a home network and sends it to a home network 30 through a roaming bound network 20. The network 30 decodes cipher with a secret key Ksa, acquires the MSN and an authentication key Sa, which is temporarily generated with a public key Kp1 of a terminal which corresponds to the MSN. When the key Sa is notified to the network 20 and an encrypted authentication key is notified to the terminal 10, the network 30 authenticates a terminal by using a random number which is generated and using these authentication keys. When authentication is completed, the network 20 acquires a roaming number and notifies it to the terminal 10 and the network 30. The terminal 10, the networks 20 and 30 separately store the roaming number and the authentication key.



LEGAL STATUS

[Date of request for examination]	21.06.1996
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2877199
[Date of registration]	22.01.1999
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In a roaming method for roaming point networks other than the home network with which a terminal belongs to receive the mobile service which two or more entrepreneurs offer in an area different, respectively, while giving the 1st encryption key to said terminal The 1st decode key which decodes the information enciphered by said home network with said encryption key is given. In case said terminal notifies ID of this terminal to said home network through a roaming point network The roaming method characterized by decoding ID which enciphered said ID using said 1st encryption key in said terminal, and was enciphered using said 1st decode key in said home network.
[Claim 2] The roaming method of claim 1 characterized by for said 1st encryption key being a public key, and said 1st decode key being a private key.
[Claim 3] While transmitting the authentication key which gave said 2nd decode key which decodes the information enciphered by said terminal with said 2nd encryption key while giving the 2nd encryption key to said home network, and was generated with said home network to said roaming point network The roaming method of claims 1 or 2 characterized by decoding the authentication key which enciphered said authentication key with said 2nd encryption key, transmitted to said terminal through said roaming point network, and was enciphered using said 2nd decode key in said terminal.
[Claim 4] Said roaming point network generates a random number, and this random number is transmitted to said terminal with said enciphered authentication key. The result of an operation which obtained in said terminal by performing data processing of said random number and the authentication key decoded with said 2nd decode key is made to return said roaming point network. The roaming method of claim 3 characterized by performing authentication processing by comparing with the result of having performed data processing of said random number and said authentication key with said roaming point network, and said result of an operation.
[Claim 5] The roaming method of claims 3 or 4 with which said 2nd encryption key is a public key, and said 2nd decode key is characterized by being the private key of a proper at said terminal.
[Claim 6] The roaming method of claims 3, 4, or 5 characterized by performing roaming registration about said terminal in said home network and said roaming point network using the roaming number which said roaming point network assigns to said terminal, and said authentication key.
[Claim 7] In the migration communication system which can receive the mobile service which two or more entrepreneurs offer in an area different, respectively with roaming point networks other than the home network with which a terminal belongs Said terminal enciphers own ID with the 1st encryption key at the time of roaming. With the network number of said home network A means to decode the authentication key enciphered as a means to make include in a roaming registration demand signal, and to transmit, with the 2nd encryption key contained in the received authentication demand signal, Have a storage means to associate and memorize the roaming number contained in the received roaming reception signal, and said authentication key, and said said roaming point network receives said roaming registration demand signal. A means to transmit the roaming demand signal between networks containing said enciphered ID to said home network which said network number shows, A means to

associate and memorize the authentication key contained in the roaming reply signal between networks from said home network, and the roaming number assigned to said terminal and to memorize, A means to transmit to said terminal by making into said authentication demand signal the authentication key enciphered with the 2nd encryption key contained in said roaming reply signal between networks, A means to transmit said roaming number to said terminal and said home network, A means by which said home network receives said roaming demand signal between networks, and decodes said enciphered ID, A means to transmit said roaming reply signal between networks which generates said authentication key, enciphers this authentication key with said 2nd encryption key corresponding to said ID, and contains said authentication key and said enciphered authentication key, Migration communication system characterized by having a storage means to relate said roaming number to said ID, and to memorize it.

[Claim 8] A random-number generation means by which said roaming point network generates the random number transmitted to said authentication demand signal by including, A comparison means to compare with the output of this operation means and the authentication reply signal from said terminal an operation means to perform the operation of said random number and said authentication key, An operation means by which have the means which assigns a roaming number to said terminal when the comparison result of this comparison means is in agreement, and said terminal performs the operation of said random number and said decoded authentication key, Migration communication system characterized by having a means to transmit to said roaming point network by making the result of an operation of this operation means into said authentication reply signal.

[Claim 9] Migration communication system of claims 7 or 8 characterized by for said 1st encryption key being a public key of said home network proper, and said 2nd-fish encryption key being a public key of said terminal proper.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] Especially this invention relates to a roaming method when a migration communication terminal moves to the service area of entrepreneurs other than the entrepreneur who contracted about a roaming method.
[0002]
[Description of the Prior Art] In the field of mobile communication, two or more entrepreneurs offer each service in an area different, respectively. and it is the migration communication terminal a contract of was made with one of entrepreneurs, it is alike and sets also in the service area which other entrepreneurs offer, and the entrepreneur of these plurality is performing roaming service so that the same service as the case where it is located in the service area of the entrepreneur who the end of a local made a contract of can be received.
[0003] With reference to drawing 5 , the registration procedure of the roaming terminal in the conventional migration terminal roaming method is explained. The roaming terminal has received the information information from a base transceiver station, and gets to know having carried out roaming between networks from the information information. That is, it gets to know having come out of the service area of the home network which the end of a local has made a contract of, and having gone into other entrepreneurs' (roaming point network) service area. And a roaming terminal transmits the location registration demand signal 501 to a roaming point network. The subscriber's number (following, MSN) which is Subscriber ID is contained in this location registration demand signal 501.
[0004] With a roaming point network (exchange), if the location registration demand signal 501 from a roaming terminal is received, it will be recognized as the terminal being a roaming terminal by MSN contained in it. And a roaming point network transmits the network authentication information read-out demand signal 502 from MSN to the home network which carried out learning, in order to perform authentication processing. MSN is contained in this network authentication information read-out demand signal 502. Moreover, a roaming point network transmits the authentication demand signal 503 to a roaming terminal. The authentication random number generated within the net [roaming point] is contained in this authentication demand signal 503.
[0005] If the home network (exchange) has memorized all authentication keys required for authentication of the terminal which belongs to a self-network and the network authentication information read-out demand signal 502 is received, it will search the authentication key of the terminal with which MSN contained in the signal was given. And the network authentication information read-out reply signal 504 notifies the searched authentication key to a roaming point network.
[0006] Moreover, if the authentication demand signal 503 is received from a roaming point network, a roaming terminal will perform an operation with the authentication key of the proper memorized with the authentication random number contained in the authentication demand signal 503, and confidence using an arithmetic circuit, and will return the result of an operation to a roaming point network with the authentication reply signal 505.

[0007] With a roaming point network, data processing of the authentication key obtained with the network authentication information read-out reply signal 504 from a home network and the same authentication random number as having transmitted to the roaming terminal previously is performed. And a roaming point network compares the result of an operation with the authentication result of an operation contained in the authentication reply signal 505 from a roaming terminal. If these results are in agreement, it will be judged with a roaming terminal being a terminal registered into the home network. That is, it becomes Authentication O.K. And a roaming point network catches the roaming number (ROM) which should be given to the roaming terminal, and transmits the location registration reception signal 506 containing ROM to a roaming terminal. Moreover, a roaming point network transmits the location registration demand signal 507 between networks containing MSN and RON to a home network.

[0008] A home network will memorize MSN and RON which are contained in the signal, if the location registration demand signal 507 between networks is received from a roaming point network. And the information about the terminal corresponding to MSN, for example, subscriber information, an authentication key, etc. are transmitted with the location registration reply signal 508 between networks.

[0009] A roaming point network is memorized with RON which assigned the subscriber information included in the location registration reply signal 508 between networks transmitted from the home network, and information, such as an authentication key, to the roaming terminal.

[0010] By the conventional roaming method, registration processing of a roaming terminal is performed as mentioned above. Call processing at the time of call origination is henceforth performed directly between a roaming point network and a roaming terminal from this at the time of the location registration of a roaming terminal.

[0011] As explained above, in order to perform authentication processing of a roaming terminal efficiently, by the conventional roaming processing, the authentication key of the roaming terminal concerned is transmitted to the roaming point network from the home network at the time of first-time roaming registration. For this reason, a roaming point network will get to know an authentication key, and there is a problem in the conventional roaming method in respect of security -- there is risk, such as leakage.

[0012] There is an approach indicated by JP,4-352525,A as an approach of solving this problem. First, this generates the temporary qualification key which the roaming point network which received the location registration demand from the roaming terminal uses for roaming processing, and transmits to the home network. A home network attests a roaming terminal via a roaming point network. The home network holds the same key as the temporary authentication key setting key which a roaming terminal holds, enciphers a temporary qualification key after authentication termination using this key, and sends it to a roaming terminal via a roaming point network. A roaming terminal decodes the enciphered temporary qualification key with a temporary authentication key setting key, and obtains a temporary authentication key. Henceforth, this temporary authentication key is used for authentication processing with a roaming point network. In this way, roaming processing (authentication processing) can be performed, without an authentication key being known by the roaming point network.

[0013]

[Problem(s) to be Solved by the Invention] By the conventional roaming method, in order for a roaming terminal to perform a location registration demand, a subscriber's number (MSN) must be first transmitted to a roaming point network. Naturally, since a roaming terminal performs the transmission by wireless, it has a possibility that it may be monitored and has the trouble that the anonymity of a roaming terminal is not securable.

[0014] This invention aims at offering the roaming method which performs roaming processing and which can carry out things, without notifying the information on a subscriber's number and terminal propers, such as an authentication key, to a roaming point network.

[0015] Moreover, this invention aims at building the high migration communication system of security.

[0016]

[Means for Solving the Problem] While giving the 1st encryption key to said terminal in a roaming

method for roaming point networks other than the home network with which a terminal belongs to receive the mobile service which two or more entrepreneurs offer in an area different, respectively according to this invention The 1st decode key which decodes the information enciphered by said home network with said encryption key is given. In case said terminal notifies ID to said home network through a roaming point network The roaming method characterized by decoding ID which enciphered and notified said ID using said 1st encryption key in said terminal, and was enciphered using said 1st decode key in said home network.

[0017] Moreover, while giving the 2nd encryption key to said home network according to this invention While transmitting the authentication key which gave said 2nd decode key which decodes the information enciphered by said terminal with said 2nd encryption key, and was generated with said home network to said roaming point network Said authentication key is enciphered with said 2nd encryption key, it transmits to said terminal through said roaming point network, and the roaming method characterized by decoding the authentication key enciphered using said 2nd decode key in said terminal is obtained.

[0018] If this invention is furthermore caused, said roaming point network will generate a random number, and this random number and said enciphered authentication key will be transmitted to said terminal. In said terminal, perform data processing of said random number and the authentication key decoded with said 2nd decode key, and the result of an operation is made to return said roaming point network. By said roaming point network's performing data processing of said random number and said authentication key, and comparing with said result of an operation, the roaming method characterized by performing authentication processing is obtained.

[0019] In the migration communication system which can receive the mobile service which two or more entrepreneurs offer in an area different, respectively further again according to this invention with roaming point networks other than the home network with which a terminal belongs Said terminal enciphers own ID with the 1st encryption key at the time of roaming. With the network number of said home network A means to decode the authentication key enciphered as a means to make include in a roaming registration demand signal, and to transmit, with the 2nd encryption key contained in the received authentication demand signal, Have a storage means to associate and memorize the roaming number contained in the received roaming reception signal, and said authentication key, and said said roaming point network receives said roaming registration demand signal. A means to transmit the roaming demand signal between networks containing said enciphered ID to said home network which said network number shows, A means to associate and memorize the authentication key contained in the roaming reply signal between networks from said home network, and the roaming number assigned to said terminal and to memorize, A means to transmit to said terminal by making into said authentication demand signal the authentication key enciphered with the 2nd encryption key contained in said roaming reply signal between networks, A means to transmit said roaming number to said terminal and said home network, A means by which said home network receives said roaming demand signal between networks, and decodes said enciphered ID, A means to transmit said roaming reply signal between networks which generates said authentication key, enciphers this authentication key with said 2nd encryption key corresponding to said ID, and contains said authentication key and said enciphered authentication key, The migration communication system characterized by having a storage means to relate said roaming number to said ID, and to memorize it is obtained.

[0020]

[Function] MSN contained in a roaming registration demand signal from a roaming terminal is enciphered with the public key of a home network. For this reason, MSN of a roaming terminal is not known by the third person including a roaming point network.

[0021] Moreover, the authentication key used for the authentication processing between a roaming terminal and a roaming point network is not generated by the home network, and is not the thing of a roaming terminal proper. And since the notice to a roaming terminal from a roaming point network is performed in the condition of having been enciphered with the public key of a roaming terminal proper, it is known by not any third persons other than a roaming point network.

[0022]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing. First, with reference to drawing 1 thru/or drawing 3 , the configuration of the roaming terminal which adopts the roaming method of this invention, a roaming point network, and a home network is explained.
[0023] Drawing 1 is the block diagram of the roaming terminal 10. This roaming terminal 10 has read-only memory (following, ROM) 11a, memory (following, RAM) 11b which can be written in and 1st operation part 12a, the 2nd operation part 12b, and the wireless transceiver section 13. Moreover, it has the control section which controls these and which is not illustrated.
[0024] ROM11a has memorized the subscriber (ID) number (following, MSN) assigned to the terminal, the private key of a terminal proper and the network number of a home network, the public key of a home network, etc. In case RAM11b performs roaming processing, it memorizes the authentication key delivered from a home network. Moreover, 1st operation part 12a performs the operation by the public key authentication method, and 2nd operation part 12b performs the operation by the private key authentication method.
[0025] Drawing 2 is the block diagram of the roaming point network (exchange) 20. This roaming point network 20 has the ** area location register (following, VLR) 21, operation part 22, wireless transceiver section 23a, communications control section 23b, the call control section 24, PN oscillation section 25, and a comparator 26.
[0026] VLR21 stores a roaming subscriber's roaming number (the following, RON), an authentication key, positional information, etc. Operation part 22 is the same algorithm as 1st operation part 12a of the roaming terminal 10, and performs data processing of a private key authentication method. Wireless transceiver section 23a is an interface with other networks with which an interface with a base transceiver station (not shown) and communications control section 23b contain the home network of the roaming terminal 10. Moreover, the call control section 24 performs call controls, such as roaming processing between terminals, and authentication processing. PN oscillation section 25 generates a random number. A comparator 26 judges an authentication result.
[0027] Drawing 3 is the block diagram of the home network (exchange) of the roaming terminal 10. This home network 30 has home location register (following, HLR) 31a, RAM31b, operation part 32, the communications control section 33, the call control section 34, and the authentication key generation section 35.
[0028] HLR31a has memorized MSN of two or more terminals (a roaming terminal is included) which belongs to a self-network, the public key of each terminal, etc. RAM31b has memorized the private key of the home network 30. Operation part 32 is the same algorithm as operation part 12b of the roaming terminal 10, and performs data processing of a public key authentication method. The communications control section 33 is an interface with the other networks containing the roaming point network 20. The call control section 34 processes a call. The authentication key generation section 35 generates the authentication key used for the authentication processing between the roaming terminal 10 and the roaming point network 20.
[0029] Hereafter, the roaming method in the system containing these roaming terminal 10, the roaming point network 20, and the home network 30 is explained also with reference to drawing 4 .
[0030] The migration communication terminal recognizes the location where the end of a local exists using the information information always sent from a mobil radio communication network, when it is in the area where mobile service is offered. Therefore, a migration communication terminal can recognize having entered in the service area which entrepreneurs other than the entrepreneur who the end of a local made a contract of offer, i.e., having become the roaming terminal 10.
[0031] The control section of the roaming terminal 10 will read the public key (following, Kpa) of the network number (the following, NW1) of a home network, MSN, and a home network from ROM11a, if it recognizes that the end of a local carried out roaming to the roaming point network 20 using information information. And the public key authentication operation which used MSN and Kpa for operation part 12b is performed, and the result of an operation {the following and Kpa (MSN)} is

obtained. That is, using Kpa, operation part 12b enciphers MSN and obtains Kpa (MSN). And a control section sends out the roaming registration demand signal 401 containing NW1 and Kpa (MSN) to the roaming point network 20 through the wireless transceiver section 13.

[0032] With the roaming point network 20, the call control section 24 receives the roaming registration demand signal 401 through wireless transceiver section 23a. And the call control section 24 recognizes that the home network of the roaming terminal 10 is the home network 30 from NW1 contained in the roaming registration demand signal 401. And the call control section 24 sends out the roaming demand signal 402 between networks containing Kpa (MSN) contained in the received roaming registration demand signal 401 to the home network 30.

[0033] With the home network 30, the call control section 34 receives the roaming demand signal 402 between networks through the communications control section 33. The private key (following, Ksa) of a home network will be read from RAM31b, and the call control section 34 will be supplied to operation part 32 with Kpa (MSN) which received, if the roaming demand signal 402 between networks is received. Operation part 32 performs public key authentication data processing by Kpa (MSN) and Ksa. That is, operation part 32 decodes Code Kpa (MSN) using Ksa, and obtains MSN of the roaming terminal 10. The call control section 34 takes out the public key Kp1 of the roaming terminal 10 from HLR31a based on MSN obtained by operation part 32. The call control section 34 directs generation of an authentication key to coincidence to the authentication key generation section 35. With the directions from the call control section 34, the authentication key generation section 35 is the approach of arbitration, generates a temporary authentication key (following and Sa), and is Sa to the call control section 34. It notifies.

[0034] Then, the call control section 34 is Kp1 and Sa which were obtained as mentioned above. It notifies to operation part 32. Operation part 32 is Kp1 and Sa. Public key data processing is performed and the result of an operation {the following and Kp1 (Sa)} is obtained. That is, operation part 32 is Sa. It enciphers by Kp1. The call control section 34 is this Kp1 (Sa) and the original Sa. The roaming reply signal 403 between networks to include is returned to the roaming point network 20 through the communications control section 33.

[0035] If the roaming reply signal 403 between networks is returned from the home network 30 with the roaming point network 20, the call control section 24 is Kp1 (Sa) and Sa. It takes out. And the call control section 24 is the random number Rn generated in Kp1 (Sa) and PN oscillation section 25. The authentication demand signal 404 to include is sent out to the roaming terminal 10.

[0036] At the roaming terminal 10, if the authentication demand signal 404 is received, a control section will read the private key (the following, Ks1) of a proper from ROM11a. And operation part 12b is made to perform data processing of Kp1 (Sa) and Ks1. That is, operation part 12b decodes Kp1 (Sa) using Ks1, and obtains the result of an operation (following, Sa'). Furthermore, a control section is [obtained Sa' and] the random number Rn received previously. Operation part 12a is made to perform used data processing. If it puts in another way, operation part 12a is a random number Rn. It enciphers by Sa' and result-of-an-operation RES' is obtained. A control section transmits to the roaming point network 20 through the wireless transceiver section 13 by making this RES' into the authentication reply signal 405.

[0037] It is a random number Rn by the operation part 22 after transmitting the authentication demand signal 404 with the roaming point network 20. Authentication key Sa Data processing is performed and the result of an operation RES is called for. This result of an operation RES is given to a comparator 26, and is compared with result-of-an-operation RES' contained in the authentication reply signal 405 transmitted from the roaming terminal 10. When these are in agreement as a result of a comparison, the call control section 24 judges with Authentication O.K., and directs assignment of RON to the roaming terminal 10 to VLR21. Moreover, in the case of an inequality, the call control section 24 judges with Authentication NG, and stops call connection processing.

[0038] The call control section 24 which received the notice of RON from VLR21 transmits the roaming registration reception signal 406 containing RON to the roaming terminal 10 through wireless transmitting section 23a. Moreover, the call control section 24 is RON and Sa. The roaming registration

demand signal 407 between networks to include is transmitted to the home network 30 through communications control section 23b.

[0039] At the roaming terminal 10, if the roaming registration reception signal 406 is received, a control section stores RON contained in the received signal, and Sa' for which it asked by the previous operation in RAM11b.

[0040] Sa by which the call control section 34 is contained in this signal with the home network 30 when the roaming registration demand signal 407 between networks is received RON is related with previous MSN and stored in HLR21. And the call control section 34 transmits the roaming registration reception signal 408 between networks which shows that registration was received to the roaming point network 20.

[0041] The call control section 24 of the roaming point network 20 is RON and Sa if the network registration reception signal 408 is received. It stores in VLR21.

[0042] Registration processing (roaming processing) of a roaming terminal is completed as mentioned above. Then, connection processing at the time of the dispatch from the roaming terminal 10 and the arrival to the roaming terminal 10 is performed as follows.

[0043] When performing dispatch (call origination) from the roaming terminal 10, the roaming terminal 10 sends out the dispatch demand signal containing RON to the roaming point network 20.

[0044] The roaming point network 20 will recognize that the terminal which is demanding call origination is a roaming terminal by RON contained in this signal, if the dispatch demand signal from a terminal is received. And the roaming point network 20 is the authentication key Sa of the terminal corresponding to RON from VLR21. It takes out and is this authentication key Sa. It uses and authentication processing is performed. And after authentication processing is completed normally, it shifts to call connection processing.

[0045] Moreover, when there is arrival to the roaming terminal 10, the home network 30 recognizes that the corresponding terminal is among roaming from RON stored in HLR31a. And the home network 30 notifies a call in to the roaming point network 20. RON is set to the arrival-of-the-mail address of the notice signal used for this notice.

[0046] the positional information of the terminal corresponding to [based on the notice signal from the home network 30] RON from VLR21 in the roaming point network 20, and authentication key Sa etc. -- information is taken out and arrival-of-the-mail connection processing is performed.

[0047]

[Effect of the Invention] If this invention is caused, even if monitored in the wireless section, it will not be exposed of MSN by enciphering MSN transmitted to a home network through a roaming point network with the public key of a home network, and having made it transmit from a roaming terminal. And it can be made secret also to a roaming point network.

[0048] moreover, as for the authentication key transmitted to a roaming point network from a home network, since it is what is not a thing of a proper and was temporarily generated with the home network to the terminal, even if an authentication key is revealed with a roaming point network, 7 does not have a big problem on security.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram of the roaming terminal with which the roaming method of this invention is applied.
[Drawing 2] It is the block diagram of the roaming point network with which the roaming method of this invention is applied.
[Drawing 3] It is the block diagram of the home network with which the roaming method of this invention is applied.
[Drawing 4] It is drawing showing the gestalt of 1 operation of the roaming method of this invention.
[Drawing 5] It is drawing for explaining the procedure of roaming terminal registration processing of the conventional roaming method.
[Description of Notations]
10 Roaming Terminal
11a Read-only memory (ROM)
11b Memory which can be written in (RAM)
12a The 1st operation part
12b The 2nd operation part
13 Wireless Transceiver Section
20 Roaming Point Network
21 ** Area Location Register (VLR)
22 Operation Part
23a Wireless transceiver section
23b Communications control section
24 Call Control Section
25 PN Oscillation Section
26 Comparator
30 Home Network
31a Home location register (HLR)
31b RAM
32 Operation Part
33 Communications Control Section
34 Call Control Section
35 Authentication Key Generation Section
401 Roaming Registration Demand Signal
402 Roaming Demand Signal between Networks
403 Roaming Reply Signal between Networks
404 Authentication Demand Signal
405 Authentication Reply Signal
406 Roaming Registration Reception Signal

407 Roaming Registration Demand Signal between Networks
408 Roaming Registration Reception Signal between Networks
501 Location Registration Demand Signal
502 Network Authentication Information Read-out Demand Signal
503 Authentication Demand Signal
504 Network Authentication Information Read-out Reply Signal
505 Authentication Reply Signal
506 Location Registration Reception Signal
507 Location Registration Demand Signal between Networks
508 Location Registration Reply Signal between Networks

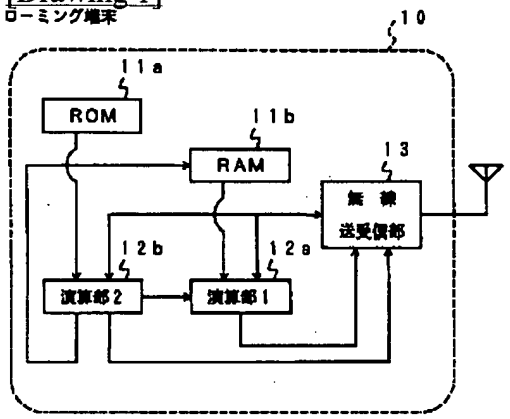
[Translation done.]

* NOTICES *

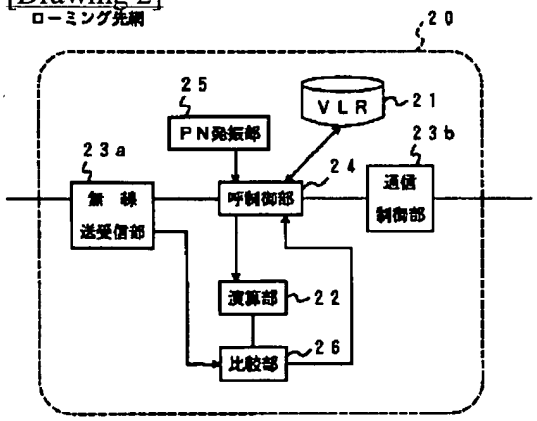
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

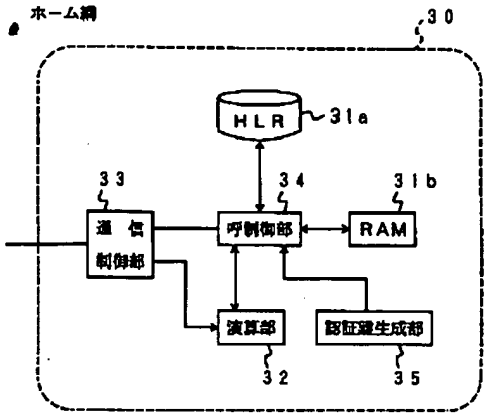
[Drawing 1]



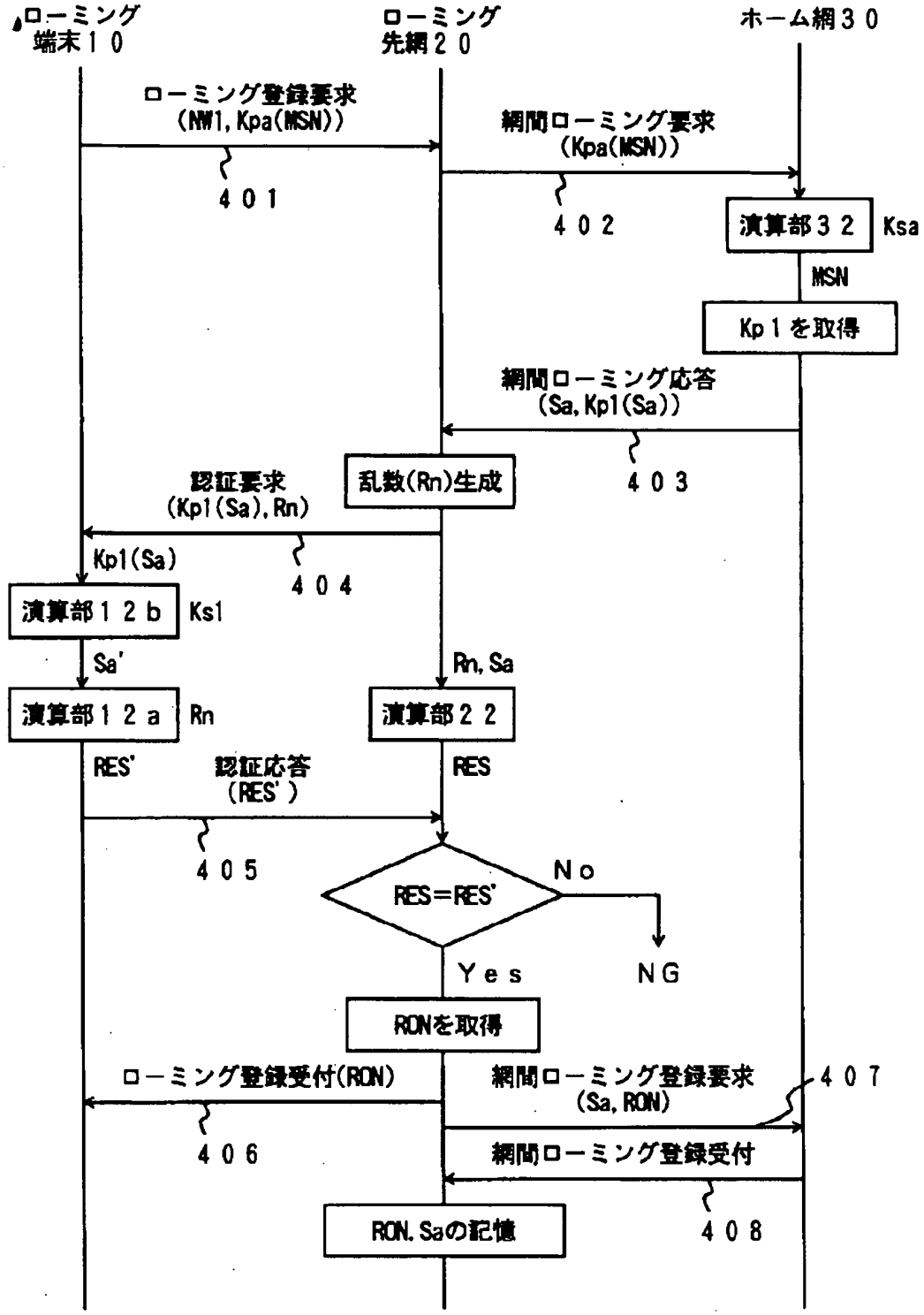
[Drawing 2]



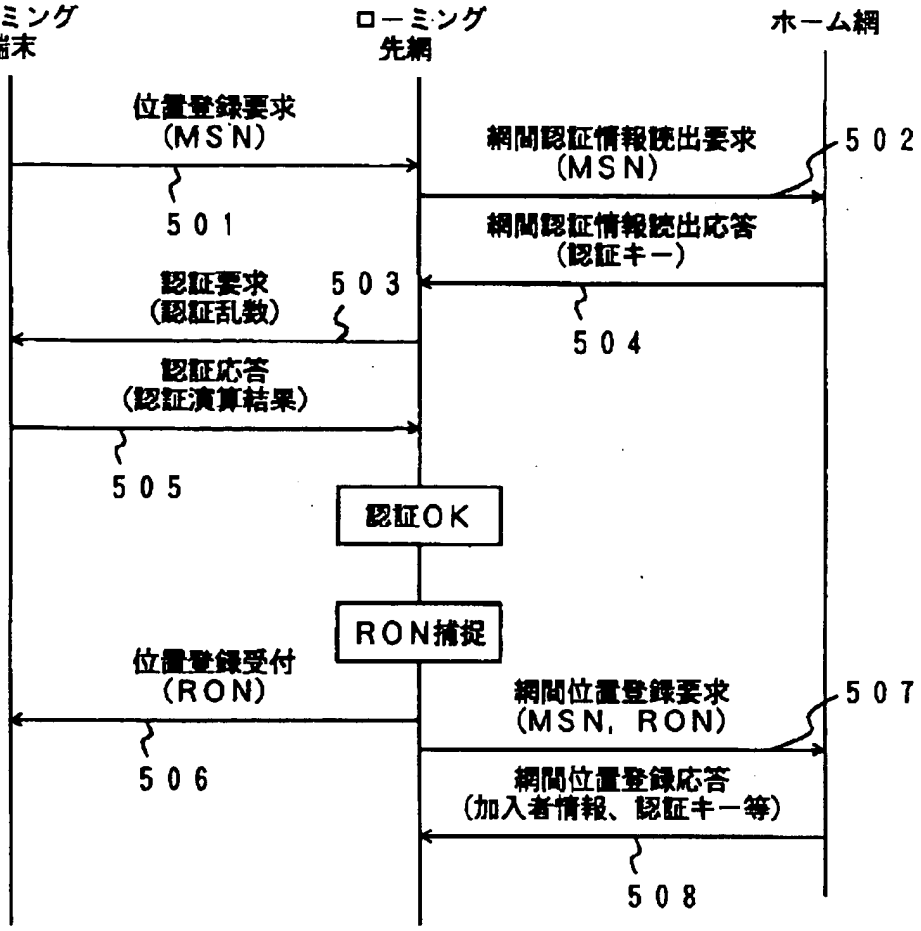
[Drawing 3]



[Drawing 4]


ローミング端末１０
ローミング先網２０
ホーム網３０
ローミング登録要求 (NW1, Kpa(MSN))
401
網間ローミング要求 (Kpa(MSN))
402
演算部３２ Ksa
MSN
Kp１を取得
網間ローミング応答 (Sa, Kp1(Sa))
403
乱数(Rn)生成
認証要求 (Kp1(Sa), Rn)
404
Kp1(Sa)
演算部１２ｂ Ks1
Sa'
Rn, Sa
演算部１２ａ Rn
演算部２２
RES'
認証応答 (RES')
RES
405
RES=RES'
No
NG
Yes
RONを取得
ローミング登録受付(RON)
406
網間ローミング登録要求 (Sa, RON)
407
網間ローミング登録受付
408
RON, Saの記憶

[Drawing 5]



[Translation done.]